

# A TEST FOR MONOMIAL CONTAINMENT

SIMON KEICHER AND THOMAS KREMER

**ABSTRACT.** We present an algorithm to decide whether a given ideal in the polynomial ring contains a monomial without using Gröbner bases, factorization or sub-resultant computations.

## 1. INTRODUCTION

Let  $\mathbb{K}$  be a field. Given an ideal  $I \subseteq \mathbb{K}[T_1, \dots, T_r]$ , the *monomial containment problem* is to decide whether  $I$  contains a monomial. Equivalently, one is interested in whether the intersection  $V(I) \cap \mathbb{T}^r$  of the zero set  $V(I) \subseteq \overline{\mathbb{K}}^r$  with the algebraic torus  $\mathbb{T}^r := (\overline{\mathbb{K}}^*)^r$  is empty. The monomial containment problem occurs frequently when determining tropical varieties [4] or when determining GIT-fans [10]. The usual approach is via Gröbner bases:  $I$  contains a monomial if and only if the saturation  $I : (T_1 \cdots T_r)^\infty$  contains  $1 \in \mathbb{K}[T_1, \dots, T_r]$ . This can also be decided by a radical membership test:  $I$  contains a monomial if and only if  $T_1 \cdots T_r \in \sqrt{I}$ .

In the present paper, we provide a direct approach involving neither Gröbner basis computations nor (sub-)resultants or factorization of polynomials. We consider more generally the following problem: given a polynomial  $g \in \mathbb{K}[T_1, \dots, T_r]$ , prove or disprove the existence of an element  $x \in \overline{\mathbb{K}}^r$  such that

$$(1) \quad f(x) = 0 \quad \text{for all } f \in I, \quad g(x) \neq 0.$$

Clearly, setting  $g := T_1 \cdots T_r \in \mathbb{K}[T_1, \dots, T_r]$  in (1), the existence of such  $x$  is equivalent to the monomial containment problem. Our algorithm, Algorithm 4.1, proceeds in three steps:

- (i) Compute finite subsets  $S_1, \dots, S_m \subseteq \mathbb{K}[T_1, \dots, T_r]$  that are in *triangular shape* and polynomials  $g_1, \dots, g_m$  such that the solutions of (1) are preserved, i.e., the zero sets satisfy

$$V(I) \setminus V(g) = \bigcup V(S_i) \setminus V(g_i) \subseteq \overline{\mathbb{K}}^r.$$

- (ii) Making certain variables  $T_j$  invertible, we obtain a function field  $\mathbb{L}$  and an embedding  $\iota: \mathbb{K}[T_1, \dots, T_r] \rightarrow \mathbb{L}[T_{k_1}, \dots, T_{k_s}]$  such that the embedded equations  $\iota(S_i)$  are *dense*, i.e., each variable  $T_{k_j}$  corresponds to an equation.
- (iii) Then an element  $x \in \overline{\mathbb{K}}^r$  satisfying (1) exists if and only if the minimal polynomial of the class  $\overline{\iota(g_i)} \in \mathbb{L}[T_{k_1}, \dots, T_{k_s}]/\langle S_i \rangle$  is not a monomial for some  $i$ .

Experiments with our implementation of Algorithm 4.1 suggest that it is competitive for certain classes of input; for instance, it usually beats the Gröbner basis approach when a solution exists, i.e., the ideal is monomial-free.

Note that the idea behind step (i) of the algorithm is quite common and similar concepts have been used by several authors for a more explicit study or even the explicit computation of solutions. See, e.g., [1, 2, 5, 8, 17] for a series of papers with

---

2010 *Mathematics Subject Classification.* 13P05, 13P10, 13P15, 14Q99 .  
The first author was supported by the DFG Priority Program SPP 1489.

Gröbner basis-free algorithms for systems of equations. The methods of Wang [16], Thomas [13, 14] as well as Bächler, Gerdt, Lange-Hegemann and Robertz [3] can also deal with systems of equations and inequalities. They determine the solutions of such systems by means of certain triangular sets called *simple systems*; their computation involves sub-resultant computations. All algorithms, including ours in step (i), share the concept of *triangular sets*, certain finite subsets  $S_i \subseteq \mathbb{K}[T_1, \dots, T_r]$  such that  $V(I) = \bigcup V(S_i)$  holds. The  $S_i$  then give insight into the structure of the solution set  $V(I) \subseteq \overline{\mathbb{K}}^r$ . As we are only interested in solvability of (1), we will only need triangular sets with weaker properties but which can be computed more efficiently.

The structure of this paper is as follows. In Section 2, we show how to decompose the given ideal into a list of triangular sets with sufficient properties for our solvability test; this is step (i) in the previous list. Section 3 is devoted to steps (ii) and (iii), i.e., we show how to reduce the problem to a dense system over a function field and how to determine the solvability of such a system by means of minimal polynomial computations. Explicit algorithms are given in each section. In Section 4, we present our algorithm for the monomial containment problem. We compare the experimental running time of the `perl` implementation [12] of the algorithm to the Gröbner basis approach as well as to the methods of [3, 16].

This paper builds on [11]. We would like to thank Jürgen Hausen for helpful discussions.

## 2. TRIANGULAR SHAPE

In this section, we treat item (i) of the list on page 1, i.e., we decompose a system as in (1) with an ideal  $I \subseteq \mathbb{K}[T_1, \dots, T_r]$  and a polynomial  $g \in \mathbb{K}[T_1, \dots, T_r]$  into a list of finite sets of polynomials that are in *triangular shape*. We show how to compute this decomposition by iteratively applying a set of operations that do not change the solvability of (1).

We first define the notion of *triangular shape*. In the literature, they are also called *triangular sets* [1, 2, 7, 9].

**Definition 2.1.** Fix the lexicographical ordering  $T_1 > \dots > T_r$  on  $\mathbb{K}[T_1, \dots, T_r]$ . We call polynomials  $f_1, \dots, f_s \in \mathbb{K}[T_1, \dots, T_r]$  of *triangular shape* if for each  $f_j$ , there is  $1 \leq k(f_j) \leq r$  such that

- (i) we have  $k(f_1) < \dots < k(f_s)$ ,
- (ii)  $f_j \in \mathbb{K}[T_{k(f_j)}, \dots, T_r] \setminus \mathbb{K}[T_{k(f_j)+1}, \dots, T_r]$  holds for each  $1 \leq j \leq s$ .

We denote by  $\deg_{T_i}(f)$  the  $(T_i)$ -degree of a polynomial  $f \in \mathbb{K}[T_1, \dots, T_r]$  considered as an element of the univariate polynomial ring  $\mathbb{K}[T_j; j \neq i][T_i]$ . Moreover, we write

$$\text{LC}_{k(f_i)}(f_i) \in R_{<k(f_i)} := \mathbb{K}[T_{k(f_i)+1}, \dots, T_r].$$

for the leading coefficient of the polynomial  $f_i$  considered in the ring  $R_{<k(f_i)}[T_{k(f_i)}]$ .

We now introduce the concept of *(semi-) triangular systems*. Assume  $I$  is generated by polynomials  $f_1, \dots, f_s \in \mathbb{K}[T_1, \dots, T_r]$ . We sort them into two sets (and keep track of the inequality  $g$ ): polynomials that are already in triangular shape  $\mathcal{F}_{\triangleleft}$  and remaining polynomials  $\mathcal{F}_{\square}$ .

**Definition 2.2.** A *semi-triangular system* (of equations) is a tuple  $(\mathcal{F}_{\square}, \mathcal{F}_{\triangleleft}, k, g)$  consisting of finite subsets  $\mathcal{F}_{\square}, \mathcal{F}_{\triangleleft} \subseteq \mathbb{K}[T_1, \dots, T_r]$ , an integer  $0 \leq k \leq r$  and a polynomial  $g \in \mathbb{K}[T_1, \dots, T_r]$  such that

- (i)  $\mathcal{F}_{\triangleleft}$  is of triangular shape,
- (ii) we have  $\text{LC}_{k(f)}(f) \mid g$  for all  $f \in \mathcal{F}_{\triangleleft}$ ,
- (iii) the set  $\{1, \dots, k\}$  contains  $\{k(f); f \in \mathcal{F}_{\triangleleft}\}$ ,

(iv) for all  $f \in \mathcal{F}_\square$  and each  $1 \leq i \leq k$  we have  $\deg_{T_i}(f) = 0$ .

Moreover, we call a semi-triangular system  $(\mathcal{F}_\square, \mathcal{F}_\triangleleft, k, g)$  a *triangular system* if  $\mathcal{F}_\square \subseteq \mathbb{K}$  holds.

**Example 2.3.** Define in  $\mathbb{K}[T_1, T_2, T_3]$  the subsets  $\mathcal{F}_\square := \emptyset$  and  $\mathcal{F}_\triangleleft := \{f_1, f_2, f_3\}$  where the  $f_i$  and  $k(f_i)$  are

$$\begin{aligned} f_1 &:= T_1^2 - (T_2 + T_3)T_1, & k(f_1) &= 1, \\ f_2 &:= T_2^2 - T_3, & k(f_2) &= 2, \\ f_3 &:= T_3^2 - T_3, & k(f_3) &= 3. \end{aligned}$$

Then  $\mathcal{F}_\triangleleft$  is of triangular shape and  $(\mathcal{F}_\square, \mathcal{F}_\triangleleft, 3, T_1T_2T_3)$  is a triangular system.

**Definition 2.4.** A list  $\mathcal{S}$  of semi-triangular systems is called a *triangle mush*. Two triangle mushes  $\mathcal{S}$  and  $\mathcal{S}'$  are *equivalent* if we have  $V(\mathcal{S}) = V(\mathcal{S}')$  with the *solutions*

$$V(\mathcal{S}) := \bigcup_{(\mathcal{F}_\square, \mathcal{F}_\triangleleft, k, g) \in \mathcal{S}} V(\mathcal{F}_\square \cup \mathcal{F}_\triangleleft) \setminus V(g) \subseteq \overline{\mathbb{K}}^r.$$

For the case of a single element  $\mathcal{S} = \{\mathcal{S}\}$ , we will use the same notions for  $\mathcal{S}$  instead of  $\mathcal{S}$ .

**Example 2.5.** Consider the triangle mush  $\mathcal{S} := \{(\mathcal{F}_\square, \emptyset, 0, g)\}$  in  $\mathbb{K}[T_1, \dots, T_4]$  where  $g := T_1T_2T_3$  and  $\mathcal{F}_\square$  consists of the two polynomials

$$f_1 := (T_3 - T_1)(T_3 - T_2)T_2, \quad f_2 := (T_1 + T_2 - T_3)T_4.$$

Going through the different cases, one directly verifies that  $V(\mathcal{S}) \subseteq \overline{\mathbb{K}}^4$  consists of all points  $(x_1, x_2, x_1, 0)$  and  $(x_1, x_2, x_2, 0) \in \overline{\mathbb{K}}^4$  where  $x_i \in \overline{\mathbb{K}}^*$ . We will continue this example in 4.3.

Given a triangle mush  $\mathcal{S}$ , we are interested in operations that transform  $\mathcal{S}$  into an equivalent triangle mush  $\mathcal{S}'$  that consists of triangular systems.

**Construction 2.6** (Solution-preserving operations). Let  $\mathcal{S} := \{(\mathcal{F}_\square, \mathcal{F}_\triangleleft, k, g)\}$  consist of a semi-triangular system. Each of the following operations produces an equivalent triangle mush  $\mathcal{S}'$ .

- (i) *Case-by-case analysis:* If  $f \in \mathbb{K}[T_{k+1}, \dots, T_r]$  and  $h \in \mathbb{K}[T_1, \dots, T_r]$  are such that  $g \mid h$  and  $h \mid fg$ , then one may choose

$$\mathcal{S}' := \{(\mathcal{F}_\square \cup \{f\}, \mathcal{F}_\triangleleft, k, g), (\mathcal{F}_\square, \mathcal{F}_\triangleleft, k, h)\}.$$

- (ii) *Polynomial division:* Consider  $f, h \in \mathcal{F}_\square$  and  $b \in \mathbb{K}[T_1, \dots, T_r]$  with  $b \mid g$ . Assume that for some  $j \in \mathbb{Z}_{\geq 0}$  we have

$$b^j f = ah + u, \quad a, u \in \mathbb{K}[T_{k+1}, \dots, T_r]$$

where  $b := \text{LC}_{T_{k+1}}(h)$  and  $\deg_{T_{k+1}}(u) < \deg_{T_{k+1}}(h)$ . Then we choose the triangle mush

$$\mathcal{S}' := \{(\mathcal{F}_\square \setminus \{f\} \cup \{u\}, \mathcal{F}_\triangleleft, k, g)\}.$$

- (iii) *Unused variable:* If  $k < r$  and  $\deg_{T_{k+1}}(f) = 0$  holds for each  $f \in \mathcal{F}_\square$ , then we may choose

$$\mathcal{S}' := \{(\mathcal{F}_\square, \mathcal{F}_\triangleleft, k+1, g)\}.$$

- (iv) *Sort polynomial:* If  $k < r$  holds and there is exactly one polynomial  $f \in \mathcal{F}_\square$  with  $\deg_{T_{k+1}}(f) \neq 0$  and  $\text{LC}_{k(f)}(f) \mid g$ , then we may choose

$$\mathcal{S}' := \{(\mathcal{F}_\square \setminus \{f\}, \mathcal{F}_\triangleleft \cup \{f\}, k+1, g)\}.$$

- (v) *Last polynomial*: Assume  $k < r$  and there is exactly one polynomial  $f \in \mathcal{F}_\square$  with  $\deg_{T_{k+1}}(f) \neq 0$ . For  $-1 \leq j \leq d$ , we write

$$\begin{aligned} f &= \sum_{i=0}^d a_i T_{k+1}^i, & f_j &:= \sum_{i=0}^j a_i T_{k+1}^i \in R_{<k+1}[T_{k+1}], \\ \mathcal{F}_\triangleleft^j &:= \mathcal{F}_\triangleleft \cup \{f_j\}, & \mathcal{F}_\square^j &:= (\mathcal{F}_\square \setminus \{f\}) \cup \{a_{j+1}, \dots, a_d\}. \end{aligned}$$

Then we may choose

$$\begin{aligned} \mathcal{S}' &:= \{(\mathcal{F}_\square^1, \mathcal{F}_\triangleleft^1, k+1, ga_1), \dots, (\mathcal{F}_\square^d, \mathcal{F}_\triangleleft^d, k+1, ga_d), \\ &\quad (\mathcal{F}_\square^{-1}, \mathcal{F}_\triangleleft, k+1, g)\}. \end{aligned}$$

*Proof.* One directly checks that in all cases  $\mathcal{S}'$  is a triangle mush. For (i), each  $x \in V(\mathcal{S})$  either satisfies  $f(x) = 0$  and  $g(x) \neq 0$  or we have  $f(x) \neq 0$  and  $h \mid fg$  implies  $h(x) \neq 0$ , i.e.,  $x \in V(\mathcal{S}')$ . The inclusion  $V(\mathcal{S}') \subseteq V(\mathcal{S})$  is clear from  $g \mid h$ . We come to (ii). Each  $x \in V(\mathcal{S})$  satisfies

$$u(x) = b(x)^j f(x) - a(x)h(x) = 0.$$

For the reverse inclusion, we use  $b \mid g$  to obtain  $b(x) \neq 0$ . Consequently, we may infer  $f(x) = 0$  from

$$b(x)^j f(x) = (b^j f)(x) = a(x)h(x) + u(x) = 0.$$

Operations (iii) and (iv) are clear. For (v), we define the following triangle mushes for  $0 \leq l \leq d$ :

$$\mathcal{S}_l := \{(\mathcal{F}_\square^l \cup \{f_l\}, \mathcal{F}_\triangleleft, k, g)\}, \quad \mathcal{D}_l := \{(\mathcal{F}_\square^j, \mathcal{F}_\triangleleft^j, k+1, ga_j); l < j \leq d\}.$$

Observe that by an application of operation (i), we obtain an equality of solutions

$$V(\mathcal{S}_l) = V(\{(\mathcal{F}_\square^{l-1} \cup \{f_l\}, \mathcal{F}_\triangleleft, k, g), (\mathcal{F}_\square^l \cup \{f_l\}, \mathcal{F}_\triangleleft, k, ga_l)\}).$$

As the ideal  $\langle \mathcal{F}_\square^{l-1} \cup \{f_l\} \rangle$  equals  $\langle \mathcal{F}_\square^{l-1} \cup \{f_{l-1}\} \rangle$  and by an application of operation (iv), we obtain

$$\begin{aligned} V(\mathcal{S}_l) &= V(\{(\mathcal{F}_\square^{l-1} \cup \{f_{l-1}\}, \mathcal{F}_\triangleleft, k, g), (\mathcal{F}_\square^l, \mathcal{F}_\triangleleft^l, k+1, ga_l)\}) \\ &= V(\mathcal{S}_{l-1} \cup (\mathcal{D}_{l-1} \setminus \mathcal{D}_l)). \end{aligned}$$

Adding the equations stored in  $\mathcal{D}_l$  on both sides does not change the solution set, i.e.,  $V(\mathcal{S}_l \cup \mathcal{D}_l)$  is equal to  $V(\mathcal{S}_{l-1} \cup \mathcal{D}_{l-1})$ . Iteratively, we obtain  $V(\mathcal{S}_d \cup \mathcal{D}_d) = V(\mathcal{S}_0 \cup \mathcal{D}_0)$ . Moreover, because of  $f_0 = a_0$  and operation (iii):

$$V(\mathcal{S}_0) = V((\mathcal{F}_\square^{-1}, \mathcal{F}_\triangleleft, k, g)) = V((\mathcal{F}_\square^{-1}, \mathcal{F}_\triangleleft, k+1, g)).$$

We conclude that  $V(\mathcal{S})$  equals  $V(\mathcal{S}_d \cup \mathcal{D}_d) = V(\mathcal{S}_0 \cup \mathcal{D}_0)$  which in turn is the same as the solution set  $V(\mathcal{S}')$ .  $\square$

The next algorithm transforms a triangle mush into an equivalent triangle mush consisting only of triangular systems. Given a triangular system  $(\mathcal{F}_\square, \mathcal{F}_\triangleleft, k, g)$ , the idea is to reduce  $T_{k+1}$ -degrees of an element  $f$  of the unsorted polynomials  $\mathcal{F}_\square$  by successive polynomial divisions; afterwards, we move  $f$  into the set of sorted polynomials  $\mathcal{F}_\triangleleft$ .

Given a finite set of polynomials  $\mathcal{F} \subseteq \mathbb{K}[T_1, \dots, T_r]$ , its *reduction* is a finite subset  $\text{red}(\mathcal{F}) \subseteq \mathbb{K}[T_1, \dots, T_r]$  such that

$$\begin{aligned} \text{LT}(f_1) \nmid \text{LT}(f_2) \quad &\text{for all } f_1, f_2 \in \text{red}(\mathcal{F}_\square), \\ \langle \text{LT}(\mathcal{F}) \rangle &\subseteq \langle \text{red}(\text{LT}(\mathcal{F})) \rangle, \quad \langle \mathcal{F} \rangle = \langle \text{red}(\mathcal{F}) \rangle \end{aligned}$$

where we denote by  $\text{LT}(f)$  or  $\text{LT}(M)$  the leading term of a polynomial  $f$  or set of polynomials  $M$  with respect to the ordering defined in Section 2. Computing the

reduction of  $\mathcal{F}$  means successively applying the division algorithm to the elements of  $\mathcal{F}$ , see, e.g., [6].

**Algorithm 2.7** (MakeTriangular). *Input:* a triangle mush  $\mathcal{S}$  in  $\mathbb{K}[T_1, \dots, T_r]$ .

- While there is  $S := (\mathcal{F}_\square, \mathcal{F}_\triangleleft, k, g) \in \mathcal{S}$  with  $k < r$ , do:
  - Replace  $\mathcal{F}_\square$  by its reduction  $\text{red}(\mathcal{F}_\square)$ .
  - If there is  $f \in \mathcal{F}_\square$  with  $\deg_{T_{k+1}}(f) > 0$ , then:
    - \* If there is  $h \in \mathcal{F}_\square \setminus \{f\}$  with  $\deg_{T_{k+1}}(h) > 0$ , then:
      - Perform a polynomial division of  $f$  by  $h$  in the univariate polynomial ring  $R := \mathbb{K}(T_{k+2}, \dots, T_r)[T_{k+1}]$  to obtain
 
$$f = a'h + u' \in R.$$
      - Set  $b := \text{LC}_{k+1}(h) \in \mathbb{K}[T_{k+2}, \dots, T_r]$  and  $j := \deg_{T_{k+1}}(h) + 1 \in \mathbb{Z}_{\geq 0}$ . With  $a := b^j a'$  and  $u := b^j u' \in \mathbb{K}[T_{k+1}, \dots, T_r]$  we then have
 
$$b^j f = ah + u \in \mathbb{K}[T_{k+1}, \dots, T_r].$$
      - Redefine  $\mathcal{S} := (\mathcal{S} \setminus \{S\}) \cup \{S', S''\}$  where
 
$$\begin{aligned} S' &:= (\mathcal{F}_\square \setminus \{f\} \cup \{u\}, \mathcal{F}_\triangleleft, k, bg), \\ S'' &:= (\mathcal{F}_\square \cup \{b\}, \mathcal{F}_\triangleleft, k, g). \end{aligned}$$
    - \* Otherwise, if there is no such  $h$ , then:
      - Redefine  $\mathcal{S} := (\mathcal{S} \setminus \{S\}) \cup \{S', S_1, \dots, S_d\}$  where with the notation of Construction 2.6 (v):
 
$$\begin{aligned} S' &:= (\mathcal{F}_\square^{-1}, \mathcal{F}_\triangleleft, k+1, g), \\ S_j &:= (\mathcal{F}_\square^j, \mathcal{F}_\triangleleft^j, k+1, ga_j). \end{aligned}$$
  - Otherwise, if there is no such  $f$ , then:
    - \* Redefine  $\mathcal{S} := (\mathcal{S} \setminus \{S\}) \cup \{S'\}$  where  $S' := (\mathcal{F}_\square, \mathcal{F}_\triangleleft, k+1, g)$ .
- Define  $\mathcal{S}' := \mathcal{S}$ .

*Output:*  $\mathcal{S}'$ . Then  $\mathcal{S}'$  is a triangle mush that is equivalent to  $\mathcal{S}$  and consists of triangular systems.

*Proof.* Note that we use only operations described in Construction 2.6; for instance, the replacement of  $\mathcal{S}$  by  $(\mathcal{S} \setminus \{S\}) \cup \{S', S''\}$  is an application of, first, operation (i) and then operation (ii). Therefore,  $\mathcal{S}'$  is equivalent to  $\mathcal{S}$ . As each  $S := (\mathcal{F}_\square, \mathcal{F}_\triangleleft, k, g) \in \mathcal{S}'$  satisfies  $k = r$ , each element of  $\mathcal{F}_\square$  is constant, i.e.,  $S$  is triangular.

It remains to show that Algorithm 2.7 terminates. To this end, consider the infinite digraph  $G' = (V', E')$  where  $V'$  is the set of all semi-triangular systems over  $\mathbb{K}[T_1, \dots, T_r]$  and, given vertices  $S_1, S_2 \in V'$ , the edge  $(S_1, S_2) \in E'$  exists if and only if Algorithm 2.7 replaces  $S_1$  within a single iteration of the while-loop by a triangle mush  $S'$  with  $S_2 \in S'$ . Let  $G = (V, E)$  be the subgraph induced by all semi-triangular systems that are reachable by a path starting in  $\mathcal{S}$ .

Consider a path  $(S_1, S_2, \dots)$  in  $G$ , i.e.,  $S_i \in V$  and  $(S_i, S_{i+1}) \in E$  for all  $i$ . We write  $S_i = (\mathcal{F}_\square^i, \mathcal{F}_\triangleleft^i, k_i, g_i)$ . By construction,  $k_i \leq k_{i+1} \leq r$  holds for all  $i$ . This means there is  $i_1 \in \mathbb{Z}_{\geq 1}$  such that  $k_{i+1} = k_i$  for all  $i \geq i_1$  and Algorithm 2.7 will perform the polynomial division  $b^j f = ah + u$ , i.e., operation (ii) of Construction 2.6, for each such  $S_i$ . Since always  $\deg_{T_{k_i+1}}(b) = 0$  holds, we have  $\deg_{T_{k_i+1}}(f) > \deg_{T_{k_i+1}}(u)$  and the reduction step only reduces  $T_{k_i+1}$ -degrees, the sequence

$$(N_i)_{i \geq i_1}, \quad N_i := \sum_{f \in \mathcal{F}_\square^i} \deg_{T_{k_i+1}}(f) \in \mathbb{Z}_{\geq 0}$$

is monotonically decreasing. As  $N_i \in \mathbb{Z}_{\geq 0}$  holds, this sequence either is finite or becomes stationary. Assume the latter holds, i.e., there is  $i_2 \in \mathbb{Z}_{\geq i_1}$  such that  $N_i = N_{i+1}$  is valid for all  $i \geq i_2$ . This implies, that for all  $i \geq i_2$  in the polynomial division step only the “ $b$ -part” will be added, i.e.,

$$\mathcal{F}_{\square}^{i+1} = \mathcal{F}_{\square}^i \cup \{b\}.$$

In particular, the ideal  $\langle \text{LT}(\mathcal{F}_{\square}^i) \rangle$  is contained in  $\langle \text{LT}(\mathcal{F}_{\square}^{i+1}) \rangle$  for each  $i \geq i_2$ . As  $\mathbb{K}[T_1, \dots, T_r]$  is noetherian, the chain

$$\langle \text{LT}(\mathcal{F}_{\square}^{i_2}) \rangle \subseteq \langle \text{LT}(\mathcal{F}_{\square}^{i_2+1}) \rangle \subseteq \dots$$

becomes stationary, i.e., there is  $i_3 \in \mathbb{Z}_{\geq 1}$  such that  $\langle \text{LT}(\mathcal{F}_{\square}^i) \rangle = \langle \text{LT}(\mathcal{F}_{\square}^{i+1}) \rangle$  holds for all  $i \geq i_3$ . Moreover, as  $b = \text{LC}_{k+1}(h)$  holds and  $h \in \text{red}(\mathcal{F}_{\square}^i)$ , we have

$$\text{LT}(b) \notin \langle \text{LT}(\text{red}(\mathcal{F}_{\square}^i)) \rangle \supseteq \langle \text{LT}(\mathcal{F}_{\square}^i) \rangle.$$

Then  $b$  cannot be an element of  $\mathcal{F}_{\square}^{i+1}$  for  $i \geq i_3$ , a contradiction. Thus, the sequence  $(N_i)_i$  is finite. In turn, this forces the  $(S_1, S_2, \dots)$  to be finite and acyclic.

Since each vertex  $S \in V$  is adjacent to only finitely many vertices, the previous argument shows that  $G$  is a finite tree. In particular, the while-loop in Algorithm 2.7 will be executed at most  $|G|$  times for each vertex  $S \in V$ , i.e., the algorithm terminates.  $\square$

**Remark 2.8.** Algorithm 2.7 is similar to the decomposition into *simple systems* used in [3]. Note, however, that they are interested in special properties (e.g., disjointness) of this decomposition whereas ours is weaker but needs not use operations like gcd or subresultant computations.

An example computation with Algorithm 2.7 will be performed at the end of the next section in Example 4.3.

### 3. SOLVABILITY

We now come to steps (ii) and (iii) in the list on page 1: as before, we assume we are given an ideal  $I = \langle f_1, \dots, f_s \rangle \subseteq \mathbb{K}[T_1, \dots, T_r]$  and a polynomial  $g \in \mathbb{K}[T_1, \dots, T_r]$  and want to answer the question whether there is  $x \in \overline{\mathbb{K}}^r$  satisfying (1).

Using Algorithm 2.7 of the previous section with input  $I$  and  $g$ , we obtain an equivalent triangle mush  $\mathcal{S}$  that consists of triangular systems. Note that we can replace each system  $(\mathcal{F}_{\square}, \mathcal{F}_{\triangleleft}, k, g) \in \mathcal{S}$  with  $\mathcal{F}_{\square} = \{0\}$  by the equivalent system  $(\emptyset, \mathcal{F}_{\triangleleft}, k, g)$ ; systems with  $\mathcal{F}_{\square} \cap \mathbb{K}^* \neq \emptyset$  clearly are not solvable. Then (1) can be rephrased as the question, whether there is  $x \in \overline{\mathbb{K}}^r$  such that

$$f(x) = 0 \quad \text{for all } f \in \mathcal{F}_{\triangleleft}, \quad g(x) \neq 0$$

holds for some  $(\emptyset, \mathcal{F}_{\triangleleft}, k, g) \in \mathcal{S}$ . Consequently, it suffices to present methods for the case  $\mathcal{S} = \{S\}$  of a single triangular system. Here is an overview of the steps to test whether  $V(S) \neq \emptyset$  holds:

$$\begin{array}{ccccccc} \mathbb{K}[T_1, \dots, T_r] & & \mathbb{L}[T_{k_1}, \dots, T_{k_s}] & & \mathbb{L}[T_{k_1}, \dots, T_{k_s}] & & \mathbb{L}[T_{k_1}, \dots, T_{k_s}] / \langle \mathcal{F}'_{\triangleleft} \rangle \\ \cup & & \cup & & \cup & & \cup \\ S & \xrightarrow{3.1} & \iota(S) & \xrightarrow{3.3} & (\emptyset, \mathcal{F}'_{\triangleleft}, k', g') & \xrightarrow{3.8} & \overline{g'} \\ & & \text{dense} & & \text{dense, monic} & & \text{min. polyn. monomial?} \end{array}$$

Here,  $\mathbb{L}$  is a suitable function field. The following proposition reduces the treatment of a triangular system in  $\mathbb{K}[T_1, \dots, T_r]$  to a triangular, *dense* system in  $\mathbb{L}[T_{k_1}, \dots, T_{k_s}]$ , i.e., a triangular system  $(\emptyset, \{f_1, \dots, f_s\}, k, g)$  such that the set  $\{k_1, \dots, k_s\}$  coincides with  $\{k(f_1), \dots, k(f_s)\}$ .

**Proposition 3.1** (Swap the field). *Consider a triangular system  $S := (\emptyset, \mathcal{F}_{\triangleleft}, k, g)$  in  $\mathbb{K}[T_1, \dots, T_r]$ . Write  $\mathcal{F}_{\triangleleft} = \{f_1, \dots, f_s\}$  and let  $k_i := k(f_i) \in \mathbb{Z}_{\geq 1}$  be as in Definition 2.1. Under the canonical embedding*

$$\iota: \mathbb{K}[T_1, \dots, T_r] \rightarrow \mathbb{L}[T_{k_1}, \dots, T_{k_s}], \quad \mathbb{L} := \mathbb{K}(T_i; i \notin \{k_1, \dots, k_s\})$$

*we obtain a triangular system  $\iota(S) := (\emptyset, \iota(\mathcal{F}_{\triangleleft}), s, \iota(g))$  that is dense in the polynomial ring  $\mathbb{L}[T_{k_1}, \dots, T_{k_s}]$ . Moreover, we have*

$$V(S) \neq \emptyset \iff V(\iota(S)) \neq \emptyset.$$

For the proof of Proposition 3.1 we recall from [18, Ch. VI] the generalization of evaluation homomorphisms; we will need this to control the elements in  $\overline{\mathbb{L}}$ . A *place* is a  $\overline{\mathbb{K}}$ -homomorphism  $\varepsilon: R_{\varepsilon} \rightarrow \overline{\mathbb{K}}$  with a subring  $R_{\varepsilon} \subseteq \overline{\mathbb{L}}$  such that

$$x \in \overline{\mathbb{L}} \setminus R_{\varepsilon} \implies x^{-1} \in R_{\varepsilon} \text{ and } \varepsilon(x^{-1}) = 0.$$

Given  $x \in \overline{\mathbb{K}}^{r-s}$ , denote by  $\varepsilon'_x: \overline{\mathbb{K}}[T_i; i \notin \{k_1, \dots, k_s\}] \rightarrow \overline{\mathbb{K}}$  the evaluation homomorphism. According to [18, Thm. 5 in VI.4], we have

$$\begin{array}{ccc} \overline{\mathbb{K}}[T_i; i \notin \{k_1, \dots, k_s\}] & \subseteq & R_{\varepsilon_x} \subseteq \overline{\mathbb{L}} \\ & \searrow \varepsilon'_x & \downarrow \varepsilon_x \\ & & \overline{\mathbb{K}} \end{array}$$

with a place  $\varepsilon_x: R_{\varepsilon_x} \rightarrow \overline{\mathbb{K}}$  extending  $\varepsilon'_x$ . Moreover, we define the *domain* of  $t = (t_1, \dots, t_s) \in \overline{\mathbb{L}}^s$  as the intersection

$$\text{Dom}(t) := \bigcap_{i=1}^s \text{Dom}(t_i), \quad \text{Dom}(t_i) := \left\{ y \in \overline{\mathbb{K}}^{r-s}; t_i \in R_{\varepsilon_y} \right\}.$$

**Lemma 3.2.** *In the situation of Proposition 3.1, assume we have  $k_1 = 1, \dots, k_s = s$ . Then the following claims hold.*

- (i) *Consider  $x \in \overline{\mathbb{K}}^{r-s}$  and  $t_1, \dots, t_n \in \overline{\mathbb{L}}$  satisfying  $\varepsilon_x(t_1 \cdots t_n) = 0$ . Then there is  $1 \leq j \leq n$  such that  $\varepsilon_x(t_j) = 0$ .*
- (ii) *For each  $t \in V(\iota(S)) \subseteq \overline{\mathbb{L}}^s$  and each  $x \in \text{Dom}(t) \subseteq \overline{\mathbb{K}}^{r-s}$ , we have  $(\varepsilon_x(t_1), \dots, \varepsilon_x(t_s), x) \in \overline{V(S)}$  where the closure is taken in  $\overline{\mathbb{K}}^r$ .*
- (iii) *Given  $x \in V(S) \subseteq \overline{\mathbb{K}}^r$ , write  $x = (x'', x')$  with  $x' \in \overline{\mathbb{K}}^{r-s}$ ,  $x'' \in \overline{\mathbb{K}}^s$ . Then there is  $t \in V(\iota(S)) \subseteq \overline{\mathbb{L}}^s$  such that*

$$x' \in \text{Dom}(t) \subseteq \overline{\mathbb{K}}^{r-s} \quad \text{and} \quad (\varepsilon_{x'}(t_1), \dots, \varepsilon_{x'}(t_s)) = x''.$$

*Proof.* For (i), we relabel  $t_1, \dots, t_n$  such that there is  $k \in \mathbb{Z}_{\geq 0}$  with  $t_i \in R_{\varepsilon_x}$  for all  $i \leq k$  and  $t_i \notin R_{\varepsilon_x}$  for  $i > k$ . By definition of places,  $\varepsilon_x(t_i^{-1}) = 0$  for all  $i > k$  and thus

$$\prod_{i=1}^k \varepsilon_x(t_i) = \varepsilon_x \left( \prod_{i=1}^n t_i \prod_{i=k+1}^n t_i^{-1} \right) = \varepsilon_x \left( \prod_{i=1}^n t_i \right) \left( \prod_{i=k+1}^n \varepsilon_x(t_i^{-1}) \right) = 0.$$

For (ii), given  $f \in \sqrt{\langle \mathcal{F}_{\triangleleft} \rangle} : g$ , we have  $\iota(f) \in \sqrt{\langle \iota(\mathcal{F}_{\triangleleft}) \rangle} : \iota(g)$ , which means  $\iota(f)(t) = 0$ . Write  $f = \sum_{\nu} a_{\nu} T^{\nu}$ . From

$$f(\varepsilon_x(t_1), \dots, \varepsilon_x(t_s), x) = \sum_{\nu} a_{\nu} \prod_{i=1}^s \varepsilon_x(t_i)^{\nu_i} \prod_{j=s+1}^r x_{j-s}^{\nu_j} = \varepsilon_x(\iota(f)(t)) = 0$$

we infer that  $(\varepsilon_x(t_1), \dots, \varepsilon_x(t_s), x) \in \overline{\mathbb{K}}^r$  is an element of the closure  $\overline{V(S)} = \overline{V(\sqrt{\langle \mathcal{F}_{\triangleleft} \rangle} : g)}$  in  $\overline{\mathbb{K}}^r$ .

We come to (iii). We first show by (finite) induction on  $0 \leq m \leq s$ , that there are  $t_{m+1}, \dots, t_s \in \overline{\mathbb{L}}$  such that for the evaluation homomorphism

$$\theta_m: \mathbb{K}[T_1, \dots, T_r] \rightarrow \overline{\mathbb{L}}[T_1, \dots, T_m], \quad T_j \mapsto \begin{cases} t_j, & m < j \leq s, \\ T_j, & \text{else} \end{cases}$$

we have  $\langle f_{m+1}, \dots, f_s \rangle \subseteq \ker(\theta_m)$  and  $\varepsilon_{x'}(t_j) = x_j$  holds for each  $m < j \leq s$ . Nothing is to prove for  $m = s$ . Assume now that this claim holds for a fixed  $1 \leq m \leq s$ ; we show that it also holds for  $m - 1$ . Since we have  $\text{LC}_m(f_i) \mid g$ ,  $g(x) \neq 0$  and  $\varepsilon_{x'}(t_j) = x_j$  for  $m < j \leq s$ , setting  $a := \text{LC}_m(f_m)$ , we obtain

$$\varepsilon_{x'}(\theta_m(a)) = a(x) \mid \varepsilon_x(g) = g(x) \neq 0.$$

In particular,  $\theta_m(a) \neq 0$ . Therefore, the non-zero univariate polynomial  $f'_m := \theta_m(f_m) \in \overline{\mathbb{L}}[T_m]$  can be decomposed into linear factors

$$f'_m = c \prod_{j=1}^n (T_m - t_{mj}) \quad \text{with } t_{mj} \in \overline{\mathbb{L}}, \quad c \in \overline{\mathbb{L}}^*.$$

Note that  $c = \theta_m(a)$  holds and thus  $\varepsilon_{x'}(c) \neq 0$ . Moreover, using again  $\varepsilon_{x'}(t_j) = x_j$  for  $j > m$  and  $f'_m = \theta_m(f_m)$ , we have  $\varepsilon_{x'}(f'_m(x_m)) = f_m(x) = 0$  where the vanishing is due to  $x \in V(S)$ . The identity

$$0 = \varepsilon_{x'}(f'_m(x_m)) = \varepsilon_{x'}\left(c \prod_{j=1}^n (x_m - t_{mj})\right)$$

together with statement (i) provide us with  $1 \leq j \leq n$  such that  $\varepsilon_{x'}(t_{mj}) = x_m$ . Defining  $t_m := t_{mj}$ , the elements  $t_m, \dots, t_s \in \overline{\mathbb{L}}$  satisfy the claims: we have  $\langle f_m, \dots, f_s \rangle \subseteq \ker(\theta_{m-1})$  since  $\theta_{m-1}(f_m) = f'_m(t_m) = 0$  and  $\varepsilon_{x'}(t_m) = x_m$  holds.

Using this argument, we now have a map  $\theta_0$  such that both  $\langle \mathcal{F}_\Delta \rangle \subseteq \ker(\theta_0)$  and  $\varepsilon_{x'}(t_m) = x_m$  hold. Setting  $t := (t_1, \dots, t_s)$ , we obtain

$$t \in V(\mathcal{F}_\Delta) \setminus V(g) = V(\iota(S)) \subseteq \overline{\mathbb{L}}$$

because  $f_m(t) = \theta_0(t_m) = 0$  for each  $1 \leq m \leq s$  and  $\varepsilon_{x'}(\theta_0(t)) = g(x) \neq 0$  implies in particular that  $\theta_0(t) = g(t) \neq 0$ . By construction,  $\varepsilon_{x'}(t) = x''$  holds.  $\square$

*Proof of Proposition 3.1.* Clearly, the system is dense. By Lemma 3.2 (iii),  $V(S) \neq \emptyset$  implies that also  $V(\iota(S))$  is non-empty. If for each  $t \in V(\iota(S))$ , there is  $x \in \text{Dom}(t)$ , then Lemma 3.2 (ii) ensures  $\overline{V(S)} \neq \emptyset$  and therefore  $V(S) \neq \emptyset$ .

It thus remains to prove that  $\text{Dom}(t) \neq \emptyset$ . Let  $1 \leq j \leq s$  be an integer. If  $t_j = 0$  holds, clearly  $\text{Dom}(t_j) = \overline{\mathbb{K}}^{r-s} \setminus V(1)$  is non-empty. If  $t_j \neq 0$ , we consider the product  $f$  of the minimal polynomial of  $t_j$  over  $\mathbb{L}$  with its common denominator and thereby obtain a polynomial  $h$ :

$$f = \sum_{i=0}^m a_i X^i, \quad h = \sum_{i=0}^m a_{m-i} X^i \in \mathbb{K}[T_j; j \notin \{k_1, \dots, k_s\}][X]$$

where  $h(t_j^{-1}) = t_j^{-m} f(t_j) = 0$ . By definition, each  $x \in \overline{\mathbb{K}}^{r-s}$  with  $x \notin \text{Dom}(t_j)$  must satisfy  $\varepsilon_x(t_j^{-1}) = 0$ . For all  $i > 0$ , from  $a_{m-i} \in \mathbb{K}[T_j; j \notin \{k_1, \dots, k_s\}]$  we know that  $a_{m-i} \in R_{\varepsilon_x}$  holds and therefore obtain  $\varepsilon_x(a_{m-i} t_j^{-i}) = 0$ . We have

$$\varepsilon_x(a_m) = \varepsilon_x\left(h(t_j^{-1}) - \sum_{i=1}^m a_{m-i} t_j^{-i}\right) = 0,$$



from which we infer that  $a_m(x) = 0$  and therefore  $x \in V(a_m) \subseteq \overline{\mathbb{K}}^{r-s}$  hold; note that the inclusion  $V(a_m) \subsetneq \overline{\mathbb{K}}^{r-s}$  is proper since  $a_m \neq 0$ . In other words,

$$\text{Dom}(t_j) \supseteq \overline{\mathbb{K}}^{r-s} \setminus V(a_m) \neq \emptyset.$$

As finite intersection of supersets of non-empty open subsets, also the set  $\text{Dom}(t) = \text{Dom}(t_1) \cap \dots \cap \text{Dom}(t_s)$  is non-empty; this completes the proof.  $\square$

For the remainder of this section, we write  $\mathbb{L}$  for a field as in Proposition 3.1; note, however, that the following claims also hold for any field  $\mathbb{L}$ .

The next step is to make all coefficients of a dense triangular system monic. We will call a triangular system  $(\emptyset, \mathcal{F}_{\triangleleft}, k, g)$  in  $\mathbb{L}[T_1, \dots, T_r]$  *monic* if  $\text{LC}_{k(f)}(f) = 1$  for all  $f \in \mathcal{F}_{\triangleleft}$ . For instance, the system in Example 2.3 is monic.

**Proposition 3.3** (Make monic). *Consider a triangular system  $S := (\emptyset, \mathcal{F}_{\triangleleft}, k, g)$  in the ring  $\mathbb{L}[T_1, \dots, T_r]$  that is dense in  $\mathbb{L}[T_n, \dots, T_r]$  for a  $1 \leq n \leq r$ . Assume there is  $f \in \mathcal{F}_{\triangleleft}$  with  $k(f) = n$  such that  $\mathcal{F} := \mathcal{F}_{\triangleleft} \setminus \{f\}$  is monic. Then the class  $\bar{h} \in R := \mathbb{L}[T_{n+1}, \dots, T_r]/\langle \mathcal{F} \rangle$  of  $h := \text{LC}_{T_n}(f)$  is annihilated by a polynomial*

$$p = bX^j + fX^{j+1} \in \mathbb{L}[X] \setminus \{0\} \quad \text{with } f \in \mathbb{L}[X], b \in \mathbb{L}^*$$

where  $j \in \mathbb{Z}_{\geq 0}$  is maximal with  $X^j \mid p$ . Moreover, writing  $f = hT_n^m + c$  with  $m \in \mathbb{Z}_{\geq 0}$  and  $c \in \mathbb{L}[T_n, \dots, T_r]$  such that  $\deg_{T_n}(c) < m$ , we have a monic dense triangular system  $S'$  that is equivalent to  $S$ :

$$S' := (\emptyset, \mathcal{F} \cup \{f'\}, k, g) \quad \text{with } f' := T_n^m - \frac{f(h)}{b}c \in \mathbb{L}[T_n, \dots, T_r].$$

**Lemma 3.4.** (i) *Consider a triangular system  $S := (\emptyset, \mathcal{F}_{\triangleleft}, k, g)$  in the ring  $\mathbb{L}[T_1, \dots, T_r]$  that is dense in  $\mathbb{L}[T_n, \dots, T_r]$  for a  $1 \leq n \leq r$ . Setting  $R := \mathbb{L}[T_n, \dots, T_r]/\langle \mathcal{F}_{\triangleleft} \rangle$ , the ring extension  $\mathbb{L} \subseteq R$  is integral.*

(ii) *Let  $\mathbb{L} \subseteq R$  be a ring extension,  $I \subseteq R$  an ideal and  $h \in R$  such that  $\bar{h} \in R/I$  is integral over  $\mathbb{L}$ . Define  $J := \sqrt{I} : h \subseteq R$  and let*

$$p = bX^j + fX^{j+1} \in \mathbb{L}[X] \quad \text{with } f \in \mathbb{L}[X], b \in \mathbb{L}^*$$

*be the minimal polynomial of  $\bar{h}$  where  $j \in \mathbb{Z}_{\geq 0}$  is maximal with  $X^j \mid p$ . Then  $h' := -f(h)/b \in R$  yields  $hh' - 1 \in J$ .*

*Proof.* For (i), we write  $\mathcal{F}_{\triangleleft} = \{f_n, \dots, f_r\}$  and assume  $k(f_i) = i$ . Define  $R_j := \mathbb{L}[T_n, \dots, T_r]/\langle f_j, \dots, f_r \rangle$  for  $n \leq j \leq r$  and  $R_{r+1} = \mathbb{L}$ . The canonical projection

$$\pi : R_{j+1}[T_j] \rightarrow R_j = R_{j+1}[T_j]/\langle \bar{f}_j \rangle, \quad f \mapsto f + \langle \bar{f}_j \rangle$$

gives us  $\pi(\bar{f}_j(T_j)) = \bar{f}_j(\bar{T}_j) = \bar{0}$ . Since  $R_j = R_{j+1}[\bar{T}_j]$  and  $\bar{f}_j \in R_{j+1}[X]$  is monic, the generator  $\bar{T}_j$  is integral over  $R_{j+1}$  and non-zero. This shows that in the chain  $R = R_n \supseteq \dots \supseteq R_{r+1} = \mathbb{L}$  each ring extension is integral, and so is  $R \supseteq \mathbb{L}$ .

We come to (ii). Note that  $p(h) \in I$  and  $I \subseteq J$  ensures  $p(h+J) = 0 + J$ . We have

$$p(\bar{h}) = (\bar{h}f(\bar{h}) + b)\bar{h}^j = \bar{0} \in R/J.$$

Observe that  $\bar{h}$  is not a zero-divisor: for each  $x \in R$  with  $xh \in \sqrt{I} : h$ , already  $x \in \sqrt{I} : h$  holds. That is  $\bar{h}f(\bar{h}) + b = \bar{0}$ . Setting  $h' := -f(h)/b$ , we obtain  $h'h - 1 \in J$  from

$$\overline{h'h - 1} = -\frac{f(h)}{b}h - 1 = -\frac{f(\bar{h})\bar{h} + b}{b} = \bar{0} \in R/J. \quad \square$$

*Proof of Proposition 3.3.* Note that the system  $(\emptyset, \mathcal{F}, k, g)$  in  $\mathbb{L}[T_1, \dots, T_r]$  is dense in  $\mathbb{L}[T_{n+1}, \dots, T_r]$ . By Lemma 3.4 (i), the residue class  $\bar{h} \in R$  is integral over  $\mathbb{L}$ ,

i.e.,  $p$  exists. Using the inclusion of the ideal  $\sqrt{\langle \mathcal{F} \rangle} : h \subseteq \mathbb{L}[T_{n+1}, \dots, T_r]$  in the ideal  $\sqrt{\langle \mathcal{F} \rangle} : g \subseteq \mathbb{L}[T_1, \dots, T_r]$ , we obtain

$$hh' - 1 \in \sqrt{\langle \mathcal{F} \rangle} : h \subseteq \sqrt{\langle \mathcal{F} \rangle} : g \quad \text{with } h' := \frac{-f(h)}{b} \in \mathbb{L}[T_{n+1}, \dots, T_r]$$

from the second statement of Lemma 3.4. One directly verifies the equality of ideals

$$\sqrt{\langle \mathcal{F}_{\triangleleft} \rangle} : g = \sqrt{\langle \mathcal{F} \rangle + \langle f \rangle} : g = \sqrt{\langle \mathcal{F} \rangle + \langle f' \rangle} : g.$$

In particular,  $V(S) = V(S')$  holds with the dense triangular system  $S'$ . Moreover,  $\text{LC}_1(f') = 1$  by choice of  $f'$  and  $S'$  is monic.  $\square$

In order to make Proposition 3.3 computational, we first show how one can compute the required minimal polynomials.

**Algorithm 3.5** (MinimalPolynomial). *Input:* an element  $g \in R$  where  $\mathbb{L} \subseteq R$  is an integral ring extension of finite dimension  $d := \dim_{\mathbb{L}}(R)$ .

- Choosing a suitable  $\mathbb{L}$ -vector space basis of  $R$ , we consider  $M := [g^0, \dots, g^d]$  as a  $d \times (d+1)$  matrix over  $\mathbb{L}$ .
- Compute the kernel  $K := \ker(M) \neq \{0\}$ .
- Choose  $q \in K \subseteq \mathbb{L}^{d+1}$  such that  $\max(1 \leq j \leq d; q_j \neq 0)$  is minimal.
- Define  $p_g := q_0 X^0 + \dots + q_d X^d \in \mathbb{L}[X]$ .

*Output:*  $p_g \in \mathbb{L}[X]$ . This is the minimal polynomial of  $g \in R$ .

*Proof.* By construction, we have  $p(g) = Mq = 0$ . For the minimality, let  $p' = \sum_{j=0}^d q'_j X^j \in \mathbb{L}[X]$  be the minimal polynomial of  $g$ . Then  $Mq' = \sum_{j=0}^d q'_j h^j = p'(h) = 0$ , i.e.,  $q' \in K$ . By choice of  $q$ , we have

$$\deg(p') = \max(1 \leq j \leq d; q'_j \neq 0) \geq \max(1 \leq j \leq d; q_j \neq 0) = \deg(p). \quad \square$$

**Remark 3.6.** In Algorithm 3.5, the element  $q \in K$  can be computed using Gaussian elimination.

**Algorithm 3.7** (Make monic). *Input:* a triangular system  $S := (\emptyset, \mathcal{F}_{\triangleleft}, k, g)$  that is dense in  $\mathbb{L}[T_1, \dots, T_r]$ . We assume  $\mathcal{F}_{\triangleleft} = \{f_1, \dots, f_r\}$  with  $k(f_i) = i$ .

- For  $n = r$  down to 1, do:
  - Set  $\mathcal{F}_{\triangleleft}^n := \{f_i; i > n\} \subseteq \mathbb{L}[T_{n+1}, \dots, T_r]$  and define the dense triangular system  $(\emptyset, \mathcal{F}_{\triangleleft}^n, k, g)$ .
  - Decompose  $f_n = hT_n^d + c$  with  $d \in \mathbb{Z}_{\geq 1}$  and  $h \in \mathbb{L}[T_{n+1}, \dots, T_r]$ ,  $c \in \mathbb{L}[T_n, \dots, T_r]$  such that  $\deg_{T_n}(c) < d$ .
  - Use Algorithm 3.5 to compute the monic minimal polynomial  $p_h \in \mathbb{L}[X]$  of  $\bar{h} \in \mathbb{L}[T_{n+1}, \dots, T_r]/\langle \mathcal{F}_{\triangleleft}^n \rangle$ .
  - Decompose  $p_h = bX^{j+1} + aX^j$  with  $b \in \mathbb{L}[X]$ ,  $a \in \mathbb{L}^*$  by choosing  $j \in \mathbb{Z}_{\geq 0}$  maximal with  $X^j \mid p_h$ .
  - Define  $h' := -b(h)/a$ . This yields  $hh' - 1 \in \sqrt{\langle \mathcal{F}_{\triangleleft}^n \rangle} : h$ .
  - Redefine  $f_n$  as  $T_n^d + h'c \in \mathbb{L}[T_n, \dots, T_r]$ . Then  $S' := (\emptyset, \mathcal{F}_{\triangleleft}^n \cup \{f_n\}, k, g)$  is a monic triangular system that is dense in  $\mathbb{L}[T_n, \dots, T_r]$ .

*Output:*  $S'$ . Then  $S'$  is a monic triangular system that is dense in  $\mathbb{L}[T_1, \dots, T_r]$  and is equivalent to  $S$ .

*Proof.* Note that the minimal polynomial  $p_h$  exists by Lemma 3.4 (i) since the system is dense. By Lemma 3.4 (ii),  $\bar{h} \in \mathbb{L}[T_{n+1}, \dots, T_r]/\sqrt{\langle \mathcal{F}_{\triangleleft}^n \rangle} : h$  is invertible. The remaining steps are correct by Proposition 3.3.  $\square$

We now show that the existence of solutions of a monic, dense triangular system can be tested by determining a minimal polynomial.

**Proposition 3.8** (Solvability). *Let  $S := (\emptyset, \mathcal{F}_{\triangleleft}, k, g)$  be a monic triangular system that is dense in  $\mathbb{L}[T_1, \dots, T_r]$ . Set  $R := \mathbb{L}[T_1, \dots, T_r]/\langle \mathcal{F}_{\triangleleft} \rangle$ . Then  $\mathbb{L} \subseteq R$  is an integral extension and with the minimal polynomial  $p_g \in \mathbb{L}[X]$  of the residue class  $\bar{g} \in R$  we have*

$$V(S) \neq \emptyset \iff p_g \in \mathbb{L}[X] \text{ is not a monomial.}$$

**Lemma 3.9.** *In the situation of Proposition 3.8, let  $p \in \mathbb{L}[X]$  be a polynomial with  $p(g) \in \sqrt{\langle \mathcal{F}_{\triangleleft} \rangle}$ . Then there is  $k \in \mathbb{Z}_{\geq 0}$  such that  $p_g \mid p^k$ .*

*Proof.* By assumption, there is  $k \in \mathbb{Z}_{\geq 1}$  such that  $p(g)^k \in \langle \mathcal{F}_{\triangleleft} \rangle$ , i.e.,  $p^k(\bar{g}) = \bar{0} \in R$ . The monic greatest common denominator  $a := \gcd(p^k, p_g) \in \mathbb{L}[X]$  satisfies  $f(\bar{g}) = \bar{0} \in R$  since  $p^k(\bar{g}) = p_g(\bar{g}) = \bar{0}$ . By minimality of  $p_g$ , we obtain  $p_g = a \mid p^k$ .  $\square$

*Proof of Proposition 3.8.* Given  $x \in V(\mathcal{F}_{\triangleleft}) \subseteq \bar{\mathbb{L}}^r$ , the corresponding evaluation homomorphism  $\varepsilon_x$  fits into the commutative diagram

$$\begin{array}{ccc} \mathbb{L}[T_1, \dots, T_r] & \xrightarrow{\varepsilon_x} & \bar{\mathbb{L}} \\ & \searrow f \mapsto \bar{f} & \nearrow \varphi_x \\ & R & \end{array}$$

The fact, that  $\mathbb{L} \subseteq R$  is integral is Lemma 3.4 (i). Assume now  $p_g = X^n$  holds for some  $n \in \mathbb{Z}_{\geq 0}$ , i.e.,  $\bar{g} \in R$  is nilpotent. By the diagram,  $g(x) = \varphi_x(\bar{g})$  then also is nilpotent for each  $x \in V(\mathcal{F}_{\triangleleft}) \subseteq \bar{\mathbb{L}}^r$ . This means  $g(x) = 0$ .

For the reverse direction, assume  $g(x) = 0$  holds for each  $x \in V(\mathcal{F}_{\triangleleft}) \subseteq \bar{\mathbb{L}}^r$ , i.e., by the diagram, we have  $p'(g(x)) = 0$  with  $p' := X \in \mathbb{L}[X]$ . By Lemma 3.9, there is  $k \in \mathbb{Z}_{\geq 0}$  such that  $p_g \mid (p')^k = X^k$ .  $\square$

We now put the previous propositions and algorithms together to obtain an algorithm to check the existence of solutions of a triangular system. This completes steps (ii) and (iii) of the list on page 1.

**Algorithm 3.10** (IsSolvable). *Input:* a triangular system  $S = (\mathcal{F}_{\square}, \mathcal{F}_{\triangleleft}, k, g)$  in the ring  $\mathbb{K}[T_1, \dots, T_r]$ .

- If  $\mathcal{F}_{\square} \cap \mathbb{K}^*$  is non-empty, then:
  - return *false*.
- Consider the triangular system  $\iota(S)$  that is dense in  $\mathbb{L}[T_{k_1}, \dots, T_{k_s}]$  as in Proposition 3.1.
- Use Algorithm 3.7 with input  $\iota(S)$  to obtain a monic, dense and equivalent system  $S' = (\emptyset, \mathcal{F}'_{\triangleleft}, k', g')$  in  $\mathbb{L}[T_{k_1}, \dots, T_{k_s}]$ .
- Use Algorithm 3.5 to determine the minimal polynomial  $p_{g'} \in \mathbb{L}[X]$  of the residue class  $\bar{g'} \in \mathbb{L}[T_{k_1}, \dots, T_{k_s}]/\langle \mathcal{F}'_{\triangleleft} \rangle$ .
- If  $p_{g'}$  is a monomial, then:
  - return *false*.
- return *true*.

*Output:* *true* if  $V(S) \neq \emptyset$  and *false* otherwise.

*Proof.* By Proposition 3.1, Algorithm 3.5 and Algorithm 3.7,  $S'$  is equivalent, monic and dense. Proposition 3.8 delivers the stated solvability criterion.  $\square$

#### 4. MONOMIAL CONTAINMENT TEST AND EFFICIENCY

Putting together steps (i)–(iii) listed on page 1, we are now able to test whether a given ideal  $I \subseteq \mathbb{K}[T_1, \dots, T_r]$  contains some monomial  $T^\nu$ ,  $\nu \in \mathbb{Z}_{\geq 0}^r$ . Afterwards, we explore the experimental running time of the second author's implementation [12] of

the algorithm in `perl` on a series of random polynomials and compare it with Buchberger's algorithm. Moreover, we compare its efficiency on the examples `polysys50` from [15] to algorithms listed in [3, Tab. 1].

**Algorithm 4.1** (ContainsMonomial). *Input:* generators  $f_1, \dots, f_s$  for an ideal  $I \subseteq \mathbb{K}[T_1, \dots, T_r]$ .

- Define the semi-triangular system  $S := (\mathcal{F}_\square, \emptyset, 0, g)$  where  $g := T_1 \cdots T_r$ , and  $\mathcal{F}_\square := \{f_1, \dots, f_s\}$ .
- Let  $\mathcal{S}$  be the output of Algorithm 2.7 applied to  $\{S\}$ .
- For each  $S \in \mathcal{S}$ , do:
  - If Algorithm 3.10 returns *true*, then
    - \* Return *false*.
- Return *true*.

*Output:* *true* if  $T^\mu \in I$  for some  $\mu \in \mathbb{Z}_{\geq 0}^r$ . Returns *false* otherwise.

**Remark 4.2.** In the second line of Algorithm 4.1 it is more efficient to modify Algorithm 2.7 such that it checks for solutions immediately after determining a new semi-triangular system.

**Example 4.3.** In the setting of Example 2.5, we apply Algorithm 4.1 with Remark 4.2 to test whether the ideal  $I := \langle f_1, f_2 \rangle \subseteq \mathbb{K}[T_1, \dots, T_4]$  contains a monomial. To this end, we apply Algorithm 2.7 to the triangle mush  $\mathcal{S}_0$ . It will first choose the polynomial division for  $(f, h) := (f_1, f_2)$  to obtain

$$T_4 f_1 = (T_2 - T_3)T_2 f_2 - u, \quad u = (T_2^3 - T_3 T_2^2)T_4.$$

This yields a new triangle mush  $\mathcal{S}_1 := \{S', S''\}$  where  $S' := (\{f_2, u\}, \emptyset, 0, gT_4)$  and  $S'' := (\{f_1, f_2, T_4\}, \emptyset, 0, g)$ . In the next step, we obtain triangle mushes

$$\begin{aligned} \mathcal{S}_2 &:= \{(\{u\}, \{f_2\}, 1, T_4g), (\{f_1, f_2, T_4\}, \emptyset, 0, g)\}, \\ \mathcal{S}_3 &:= \{(\emptyset, \{f_2, u\}, 4, T_4g), (\{f_1, f_2, T_4\}, \emptyset, 0, g)\}. \end{aligned}$$

Algorithm 3.10 verifies that the zero-set  $V(f_2, u) \setminus V(T_4g)$  is empty by the following steps: first, Algorithm 3.7 with input  $(\emptyset, \{f_2, u\}, 4, T_4g)$  will return the monic system

$$(\emptyset, \{f_2, f_3\}, 4, T_4g), \quad f_3 := (T_2 - T_3)T_2^2.$$

As  $k(f_2) = 1$  and  $k(f_3) = 2$ , we set  $\mathbb{L} := \mathbb{K}(T_3, T_4)$  and the ring  $R := \mathbb{L}[T_1, T_2]/\langle f_2, f_3 \rangle$  is integral over  $\mathbb{L}$  with  $\mathbb{L}$ -basis  $(1, \overline{T_2}, \overline{T_2}^2)$ . We have

$$\overline{T_4g} = \overline{(T_3 - T_2)T_2T_3T_4} \in R, \quad \overline{T_4g}^2 = \overline{(T_3 - T_2)^2T_2^2T_3^2T_4^2} = \overline{0} \in R,$$

By Proposition 3.8, the algorithm may remove this triangular set, i.e., it remains to consider

$$\mathcal{S}_4 := \{(\{f_1, f_2, T_4\}, \emptyset, 0, g)\}.$$

The reduction step will remove the redundant equation  $f_2$ . The next steps provides us with

$$\mathcal{S}_5 := \{(\emptyset, \{f_1, T_4\}, 4, u'g), (\{f_1, T_4, u'\}, \emptyset, 0, g)\}, \quad u' := (T_2 - T_3)T_2.$$

By Algorithm 3.10, the system  $S := (\emptyset, \{f_1, T_4\}, 4, u'g)$  has a solution: similar to before, Algorithm 3.7 returns the monic system

$$(\emptyset, \{f_4, T_4\}, 4, u'g), \quad f_4 := T_1 - T_3$$

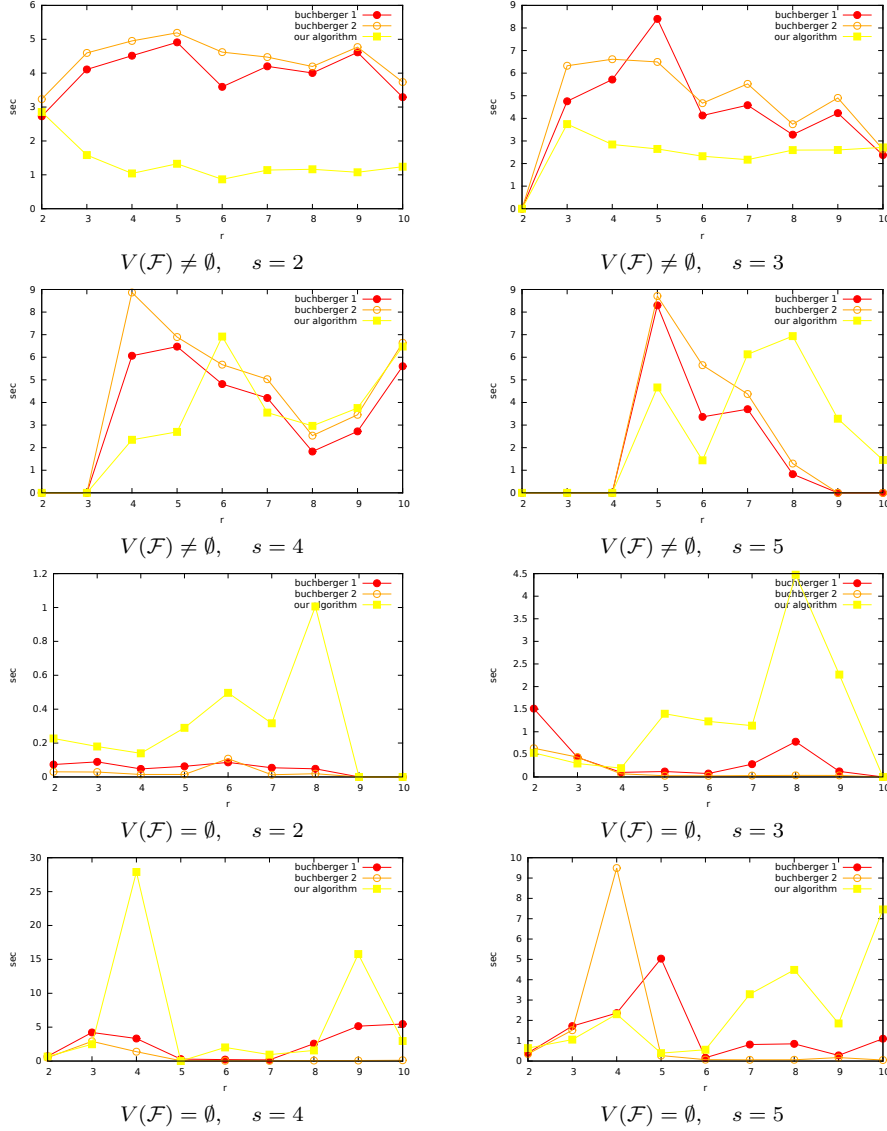
with  $k(f_4) = 1$  and  $k(T_4) = 4$ . Setting  $\mathbb{L} := \mathbb{K}(T_2, T_3)$ , the ring extension  $\mathbb{L} \subseteq R := \mathbb{L}[T_1, T_4]/\langle f_4, T_4 \rangle$  is integral with  $\mathbb{L}$ -basis  $(1)$ . Since

$$\overline{u'g} = \overline{(T_2 - T_3)T_1T_2^2T_3} = \overline{(T_2 - T_3)T_2^2T_3^2} \in R$$

is non-zero, its minimal polynomial  $p = X - (T_2 - T_3)T_2^2T_3^2 \in \mathbb{L}[X]$  is not a monomial, i.e.,  $V(S) \neq \emptyset$  by Proposition 3.8. Thus,  $\mathcal{S}_0$  has a solution as we already witnessed in Example 2.5. In particular,  $I$  contains no monomial, i.e., the algorithm returns *false*.

The remainder of this note is devoted to experimental running times. We apply the **perl** implementation [12] of Algorithm 4.1 to a series of random ideals  $\langle f_1, \dots, f_s \rangle \subseteq \mathbb{K}[T_1, \dots, T_r]$  for fixed  $2 \leq s \leq 5$  and running  $1 \leq r \leq 10$ . Moreover, setting  $\mathcal{F} := \{f_1, \dots, f_s\}$ , we distinguish the cases  $V(\mathcal{F}) = \emptyset$  and  $V(\mathcal{F}) \neq \emptyset$ .

To make the experimental running times better comparable to Buchberger's Gröbner basis algorithm [6], we have reimplemented the latter in **perl** in two variants: the first one is the classical version whereas the second one stops as soon as a monomial could be found. Both algorithms as well as the testing sets  $\mathcal{F}$  are available at [12]. The following graphics show the averages over the successful tests.



On the given set of polynomials, Algorithm 4.1 seems to be competitive when  $V(\mathcal{F}) \neq \emptyset$  whereas, for  $V(\mathcal{F}) = \emptyset$ , the classical Buchberger's algorithm usually needs less time.

Additionally, we have applied Algorithm 4.1 to the set of examples `polysys50` from [15]; its running time as well as the number of performed additions on a 2.66 GHz machine with time bound 300 seconds and at most 1 GB of RAM is listed in the left-hand side part of the following table. We write “n/a” if the computation was unsuccessful either due to time reasons or because it was out of memory.

Moreover, in the right-hand part of the table, we list some of the running times listed in [3, Table 1] on the same examples. We want to stress the fact that the two sides of this table are only marginally comparable: not only is the goal different ([3] deduces more information on the solutions whereas we test the existence of solutions), also the machines and maximal running times / memory are different.

no.	time 4.1	result	add.s	time RC1	time DW1	time AT1
1	> 300	n/a	n/a	3.5	0.4	3.0
2	> 300	n/a	n/a	7.4	7.6	7.1
3	30.89	1	4956	> 3h	985.7	7538.0
4	> 300	n/a	n/a	> 4 GB	> 4 GB	0.2
5	0.62	0	2449			
6	2.25	1	4239	0.4	0.1	0.2
7	> 1 GB	n/a	n/a	> 3h	7352.6	> 4 GB
8	0.14	1	214			
9	11.75	1	10149			
10	0.21	1	517			
11	0.17	1	361			
12	0.74	1	1909	0.5	0.3	0.4
13	0.15	1	214			
14	0.23	1	442	0.5	> 3h	1.5
15	29.82	1	6655			
16	> 300	n/a	n/a	0.9	1.4	1.8
17	> 300	n/a	n/a	6.5	4.7	75.5
18	2.34	1	4324	0.3	0.1	0.1
19	> 300	n/a	n/a	419.9	0.4	0.4
20	0.25	1	668			
21	> 300	n/a	n/a	1.6	86.6	4.5
22	> 300	n/a	n/a	0.6	1.2	1.5
23	> 300	n/a	n/a	0.4	0.1	29.5
24	> 300	n/a	n/a	1.2	1.3	1.0
25	0.25	1	537	1.2	> 3h	> 4 GB
26	1.07	0	4610			
27	1.47	1	2320			
28	9.89	1	6632			
29	0.15	1	297	0.3	0.3	0.3
30	> 300	n/a	n/a	> 4 GB	> 4 GB	45.3
31	> 1 GB	n/a	n/a	> 4 GB	> 4 GB	> 3h
32	0.41	1	1200			
33	> 1 GB	n/a	n/a	3.4	1.3	3.5
34	> 300	n/a	n/a	911.5	> 3h	> 4 GB
35	> 300	n/a	n/a	1.5	1.2	1.7
36	0.13	1	160			
37	0.27	1	633			
38	11.10	1	6878			
39	> 300	n/a	n/a	0.6	1.2	0.6
40	> 300	n/a	n/a			
41	> 300	n/a	n/a	1.5	1.5	7.0
42	0.35	1	1028			
43	> 1 GB	n/a	n/a	0.7	3.1	0.2
44	> 300	n/a	n/a	24.5	3.4	1.2
45	> 300	n/a	n/a			
46	> 300	n/a	n/a			
47	16.40	1	10465	1.3	2.8	13.0
48	0.23	1	563			
49	> 300	n/a	n/a	0.3	610.2	0.5

## REFERENCES

- [1] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *J. Symbolic Comput.*, 28(1-2):105–124, 1999. Polynomial elimination—algorithms and applications.
- [2] P. Aubry and M. Moreno Maza. Triangular sets for solving polynomial systems: a comparative implementation of four methods. *J. Symbolic Comput.*, 28(1-2):125–154, 1999. Polynomial elimination—algorithms and applications.
- [3] T. Bächler, V. Gerdt, M. Lange-Hegermann, and D. Robertz. Algorithmic Thomas decomposition of algebraic and differential systems. *J. Symbolic Comput.*, 47(10):1233–1266, 2012.
- [4] T. Bogart, A. N. Jensen, D. Speyer, B. Sturmfels, and R. R. Thomas. Computing tropical varieties. *J. Symbolic Comput.*, 42(1-2):54–73, 2007.

- [5] C. Chen, O. Golubitsky, F. Lemaire, M. Maza, and W. Pan. Comprehensive triangular decomposition. *CASC 2007, LNCS 4770, Springer-Verlag Berlin Heidelberg*, pages 73–101, 2007.
- [6] D. Cox, J. Little, and D. O’Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.
- [7] W. Decker and C. Lossen. *Computing in algebraic geometry*, volume 16 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin; Hindustan Book Agency, New Delhi, 2006. A quick start using SINGULAR.
- [8] J. F. Ritt. Differential algebra. *American Mathematical Society Colloquium Publications, AMS N. Y.*, Vol. XXXIII, 1950.
- [9] G.-M. Greuel and G. Pfister. *A Singular introduction to commutative algebra*. Springer, Berlin, extended edition, 2008. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann.
- [10] S. Keicher. Computing the GIT-fan. *Internat. J. Algebra Comput.*, 22(7):1250064, 11, 2012.
- [11] T. Kremer. Ein Radikalmitgliedschaftsalgorithmus. Diploma thesis, 2015.
- [12] T. Kremer. An Algorithm for the determination of  $\mathfrak{a}$ -faces, radical membership and monomial containment. Available at <https://www.math.uni-tuebingen.de/users/kremer/afaces/>, 2015.
- [13] J. M. Thomas. Differential systems. *AMS Colloquium Publications*, XXI, 1937.
- [14] J. M. Thomas. Systems and roots. *The William Byrd Press, INC, Richmond Virginia*, 1962.
- [15] D. Wang.  $\epsilon$ epsilon, for Maple including sets of examples. Available at <http://www-spiral.lip6.fr/~wang/epsilon/>, 2003.
- [16] D. Wang. Decomposing polynomial systems into simple systems. *J. Symbolic Comput.*, 25(3):295–314, 1998.
- [17] W.-T. Wu. Mathematics mechanization. *Mathematics and its Applications, Kluwer Academic Publishers Group*, 489, 2000.
- [18] O. Zariski and P. Samuel. *Commutative algebra. Vol. II*. Springer-Verlag, New York-Heidelberg, 1975. Reprint of the 1960 edition, Graduate Texts in Mathematics, Vol. 29.

MATHEMATISCHES INSTITUT, UNIVERSITÄT TÜBINGEN, AUF DER MORGENSTELLE 10, 72076 TÜBINGEN, GERMANY

*E-mail address:* keicher@mail.mathematik.uni-tuebingen.de

MATHEMATISCHES INSTITUT, UNIVERSITÄT TÜBINGEN, AUF DER MORGENSTELLE 10, 72076 TÜBINGEN, GERMANY

*E-mail address:* kremer@mail.mathematik.uni-tuebingen.de